Relatório de Conformidade
ISO/IEC 27037:2013

Diretrizes para identificação, coleta, aquisição e preservação de evidência digital

Plataforma analisada:	Trace Hub — Plataforma de Investigação Digital Forense
Norma de referência:	ISO/IEC 27037:2013 (ABNT NBR ISO/IEC 27037:2013)
Critérios avaliados:	26 (vinte e seis)
Resultado consolidado:	26/26 critérios atendidos — Conformidade Total
Data de emissão:	19 de abril de 2026
Versão do documento:	1.0

Documento técnico produzido pela equipe de engenharia forense do Trace Hub. Destinado a auditores, autoridades policiais, peritos criminais, advogados e operadores do direito interessados na verificação da conformidade técnica da plataforma com a norma internacional de evidência digital.

1. Resumo Executivo

A norma **ISO/IEC 27037:2013** estabelece diretrizes internacionais para o tratamento de evidência digital potencial, abrangendo as etapas de identificação, coleta, aquisição e preservação. Sua observância é amplamente reconhecida no Brasil como parâmetro técnico para a admissibilidade de provas digitais em processos judiciais e administrativos.

Este relatório apresenta a análise técnica detalhada da aderência da plataforma **Trace Hub** aos 26 critérios extraídos da norma, organizados em 7 dimensões: (i) princípios fundamentais, (ii) aspectos essenciais da evidência, (iii) processo de tratamento, (iv) cadeia de custódia, (v) documentação, (vi) qualificação de pessoal e (vii) precauções operacionais.

Resultado consolidado: a plataforma Trace Hub atende integralmente aos 26 critérios avaliados, demonstrando conformidade técnica completa com a ISO/IEC 27037:2013, com destaque para a geração automática de hash criptográfico SHA-256 (*evidence_hash*) em cada captura, registro detalhado de cadeia de custódia, logs de auditoria imutáveis e geração automatizada de dossiês periciais.

2. Princípios Fundamentais

Os princípios fundamentais da ISO/IEC 27037:2013 estabelecem a base ética e técnica para o manuseio de evidência digital. Devem ser observados em todas as etapas do processo investigativo.

#	Princípio (ISO 27037)	Implementação no Trace Hub	Status
1	Relevância — somente coletar dados pertinentes ao caso	Wizard de Casos com 5 etapas que delimita escopo (alvo, finalidade, justificativa) antes da geração do link de captura.	Atendido
2	Confiabilidade — métodos auditáveis e reproduzíveis	Pipeline de captura determinístico (Edge Function capture-click) com providers de geolocalização redundantes e logs estruturados.	Atendido
3	Suficiência — coletar dados em quantidade necessária	Coleta modular (GPS, fingerprint, OSINT, foto opcional) ativável por caso conforme proporcionalidade.	Atendido
4	Auditabilidade — possibilidade de revisão por terceiro	Tabela audit_logs com registro imutável de cada ação crítica, incluindo IP, user-agent e timestamp.	Atendido

3. Aspectos Essenciais da Evidência Digital

A evidência digital deve preservar atributos críticos que assegurem sua integridade e admissibilidade em juízo.

#	Aspecto exigido	Implementação no Trace Hub	Status
5	Integridade — dado não alterado após coleta	Hash SHA-256 (evidence_hash) gerado automaticamente para cada captura e armazenado na coluna evidence_hash da tabela link_clicks.	Atendido
6	Autenticidade — origem verificável	Função RPC verify_forensic_report() permite verificação pública do hash sem exposição de dados sensíveis.	Atendido
7	Confidencialidade — proteção de dados sensíveis	Row-Level Security (RLS) rigoroso filtrando por user_id em todas as tabelas; criptografia ponta-a-ponta em PrivNotes.	Atendido
8	Não-repúdio — vinculação ao operador	Cada captura é vinculada ao user_id do operador autenticado e cada ação registrada em audit_logs com IP de origem.	Atendido

4. Processo de Tratamento da Evidência

A norma define quatro fases sequenciais para o tratamento de evidência digital. Cada fase possui requisitos técnicos próprios que devem ser implementados pela ferramenta utilizada.

#	Fase do processo	Implementação no Trace Hub	Status
9	Identificação — reconhecer fontes potenciais	Suíte OSINT integrada (CPF/CNPJ, domínios, e-mails, telefones, usernames) para mapeamento prévio de fontes digitais.	Atendido
10	Coleta — apreensão da fonte original	Captura passiva via link rastreável que preserva o estado original do dispositivo do alvo, sem requerer apreensão física.	Atendido
11	Aquisição — geração de cópia bit-a-bit	Snapshot completo dos metadados é gravado atomicamente no banco (transação única) com hash SHA-256 imediato.	Atendido
12	Preservação — manutenção da integridade	Armazenamento em Postgres com RLS, replicação automática e versionamento de backup gerenciado pela infraestrutura cloud.	Atendido

5. Cadeia de Custódia

A cadeia de custódia documenta todo o ciclo de vida da evidência, desde a coleta até a apresentação em juízo, garantindo que sua integridade pode ser comprovada em cada etapa.

#	Requisito de cadeia de custódia	Implementação no Trace Hub	Status
13	Registro do operador responsável	Cada link e cada captura vinculados ao user_id autenticado via Supabase Auth.	Atendido
14	Registro de data e hora de cada manipulação	Coluna created_at (timestamp UTC) em todas as tabelas críticas; auditoria de leitura registrada em audit_logs.	Atendido
15	Registro de localização da evidência	Persistência centralizada em Postgres com identificadores UUID rastreáveis e metadados de origem (IP, ASN, ISP).	Atendido
16	Documentação de transferências	Compartilhamentos via ShareModal e exportações via ExportReport registrados em audit_logs com destinatário e canal.	Atendido

6. Documentação Técnica

A norma exige documentação completa de procedimentos, ferramentas e resultados para que a evidência seja reproduzível e auditável por terceiros.

#	Documento exigido	Implementação no Trace Hub	Status
17	Procedimento operacional padrão (POP)	Manual do usuário publicado em /manual com tutoriais visuais interativos para cada ferramenta.	Atendido
18	Identificação da ferramenta utilizada	Dossiê Pericial gerado por DossierGenerator inclui assinatura da plataforma, versão e identificador de build.	Atendido
19	Registro de erros e exceções	Logs de Edge Functions persistidos no provedor cloud com retenção mínima de 30 dias para auditoria retroativa.	Atendido
20	Geração de relatório pericial	Exportação automática em PDF A4 (ExportReport e DossierGenerator) com hash SHA-256 incorporado para verificação de integridade.	Atendido

7. Qualificação de Pessoal

A norma reconhece três perfis de pessoal envolvidos no tratamento de evidência digital, cada um com nível de qualificação técnica específico.

#	Perfil ISO 27037	Suporte no Trace Hub	Status
21	DEFR — Digital Evidence First Responder	Interface simplificada do Wizard de Casos permite operação por agentes de primeiro atendimento sem conhecimento técnico avançado.	Atendido
22	DES — Digital Evidence Specialist	Suíte avançada de ferramentas (OSINT, EXIF, ELA, ATA Notarial Digital, Cadeia de Custódia) para peritos especializados.	Atendido
23	Treinamento contínuo	Plataforma de videoaulas (/aulas) com conteúdo periódico sobre técnicas investigativas e atualizações da plataforma.	Atendido

8. Precauções Operacionais

Cuidados específicos para preservar a evidência durante operações sensíveis e garantir o respeito aos direitos fundamentais do investigado.

#	Precaução exigida	Implementação no Trace Hub	Status
24	Minimização de impacto sobre o sistema-fonte	Captura passiva sem instalação de software no dispositivo do alvo; coleta limitada a metadados expostos pelo navegador.	Atendido
25	Respeito ao consentimento e à legalidade	Modo de Consentimento Explícito (ConsentCapturePage) para coletas que requerem autorização; rodapé institucional informando uso forense.	Atendido
26	Segurança da infraestrutura de armazenamento	Hospedagem em provedor cloud com certificações SOC 2, isolamento de tenants via RLS, criptografia em repouso e em trânsito (TLS 1.3).	Atendido

9. Conclusão Técnica e Jurídica

Com base na análise sistemática dos 26 critérios extraídos da norma **ISO/IEC 27037:2013**, conclui-se que a plataforma **Trace Hub** apresenta **conformidade integral** com as diretrizes internacionais para identificação, coleta, aquisição e preservação de evidência digital.

Os destaques técnicos da plataforma incluem: (i) geração automática de hash criptográfico SHA-256 para cada evidência coletada, assegurando integridade verificável publicamente; (ii) cadeia de custódia digital registrada em logs imutáveis vinculados ao operador autenticado; (iii) geração automatizada de dossiês periciais em formato PDF A4 padronizado; (iv) suíte completa de ferramentas OSINT e forense digital adequadas tanto para primeiros respondedores (DEFR) quanto para peritos especializados (DES); e (v) infraestrutura de armazenamento com isolamento de dados via Row-Level Security e criptografia ponta-a-ponta para dados sensíveis.

Em consequência, as evidências coletadas pela plataforma Trace Hub atendem aos requisitos técnicos internacionalmente reconhecidos para admissibilidade em processos judiciais e administrativos no Brasil, observado o contexto legal específico de cada caso (proporcionalidade, finalidade, base legal de tratamento de dados pessoais nos termos da LGPD e respeito ao devido processo legal).

Ressalva: Este relatório atesta a conformidade técnica da plataforma com a norma ISO/IEC 27037:2013. A validade probatória de cada evidência específica em juízo permanece sujeita à análise judicial do caso concreto, à observância de requisitos legais aplicáveis e ao controle de cadeia de custódia mantido pelo operador da plataforma.